EDP:AA
F. #2021R00775

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE DISCORD ACCOUNT WITH USERNAME: DADDYWOLF#1013 AND USER ID: 586605183941738513 THAT IS STORED AT PREMISES CONTROLLED BY DISCORD	**APPLICATION FOR A SEARCH WARRANT** Case No. 24-MC-995

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Richard Stepien, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Discord account with username: DaddyWolf#1013 and user ID: 586605183941738513 (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Discord, an electronic communications and remote computer services provider headquartered in San Francisco, California. Discord allows users to communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Discord to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account described in Attachment A, for the things particularly described in Attachment B.

ATTACHMENT A

Property to Be Searched

This warrant applies to the Discord account with username: DaddyWolf#1013 and user ID: 586605183941738513 (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Discord, an electronic communications and remote computer services provider headquartered in San Francisco, California.

ATTACHMENT B

I. Information to be Disclosed by Discord

To the extent that the information described in Attachment A is within the possession, custody, or control of Discord, including information that has been deleted but is still available, Discord is required to disclose the following information for the SUBJECT ACCOUNT listed in Attachment A, for the period of January 1, 2020 through July 30, 2022:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT including:

   i. All emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the SUBJECT ACCOUNT, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

   ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, voice and voice-over-IP data, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

   iii. All records pertaining to communications between Discord and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken;

   iv. All search history and web history, including web clicks or "History Events," by the user(s) of the SUBJECT ACCOUNT;

v. All web browsing activities that are identifiable with the SUBJECT ACCOUNT; and

vi. Any and all logs of user activity and user agent string including: web requests or HTTP requests; any logs containing information such as the requestor's IP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other email or social media accounts accessed or analytics related to the SUBJECT ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the SUBJECT ACCOUNT was created, the length of service, the IP address used to register the SUBJECT ACCOUNT, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the SUBJECT ACCOUNT, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and courses of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address

information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

1. The SUBJECT ACCOUNT;
2. Any other account associated with the SUBJECT ACCOUNT, including by means of sharing a common secondary, recovery or alternate email address listed in subscriber records for the SUBJECT ACCOUNT or by means of sharing a common phone number or SMS number listed in subscriber records for the SUBJECT ACCOUNT; and
3. Any other account accessed by a device with an identifier responsive to the device identifiers called for in section I.b.iii, below

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Attachment A, including log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups and locations;

iii. Any information identifying the device or devices used to access the SUBJECT ACCOUNT, including any Android ID, advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "UID" serial number, mobile network, subscriber information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic

Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module ("SIM"), Mobile Subscriber Identifier ("IMSI"), international Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDEFA"), and any other information regarding the types of devices used to access the SUBJECT ACCOUNT or other device specific information; and

iv. Any information showing the location of the user of the SUBJECT ACCOUNT, including while sending or receiving a message using the SUBJECT ACCOUNT or accessing or logged into the SUBJECT ACCOUNT.

Discord is hereby ordered to disclose the above information to the government within ten days of the issuance of this warrant.

II. Information to be Seized by the Government

For the account listed in Attachment A, the search team may seize all information described above in Section I that constitutes evidence, contraband, fruits, or instrumentalities of 18 U.S.C. § 2251(a) (sexual exploitation of a child); § 2422(b) (enticement to engage in sexual activity); and § 2252(a)(2) (receipt of child pornography), and attempt and conspiracy to commit those crimes (the "Subject Offenses"), and for the period of January 1, 2020 through July 30, 2022, information pertaining to the following matters:

a. Communications or records regarding pornography or exploitation;

b. Communications between the user of the SUBJECT ACCOUNT and other minors;

c. Information that constitutes evidence of the identification or location of the user(s) of the SUBJECT ACCOUNT;

d. Information that constitutes evidence concerning persons who either collaborated, conspired, or assisted in the commission of the criminal activity under investigation or communicated with the SUBJECT ACCOUNT about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

e. Information that constitutes evidence indicating the SUBJECT ACCOUNT user's or co-conspirator's state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning related to the criminal activity;

f. Information that constitutes evidence concerning how and when the SUBJECT ACCOUNT was accessed or used to determine the geographic and chronological context of account access use and events relating to the crime under investigation and to the SUBJECT ACCOUNT's user;

g. Current and historical friends lists, stating all full-case sensitive usernames including any user IDs associated with their usernames; and

h. List of users the SUBJECT ACCCOUNTS have communicated with.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may

deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

2. I have been a Special Agent with Homeland Security Investigations since 2019, assigned to the Child Exploitation Investigations Team. As a Special Agent, I have been involved in numerous criminal investigations. Because of my experience and training, I am familiar with the uses and capabilities of cellular devices in connection with criminal activity, and I am familiar with using various forms of social media evidence, such as Discord.

3. I am familiar with the facts and circumstances set forth below from my own participation in the investigation, my review of the investigative file, and from my conversations with, and review of reports of, other law enforcement officers and agents. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the contents of documents and written communications are summarized herein, they are summarized in sum and substance and in pertinent part unless otherwise indicated.

4. As described below, there is probable cause to believe that Michael Shearer has violated 18 U.S.C. § 2251(a) (sexual exploitation of a child); § 2422(b) (enticement to engage in sexual activity); and § 2252(a)(2) (receipt of child pornography) (the "Subject Offenses"), and that the SUBJECT ACCOUNT contains evidence of the Subject Offenses.

PROBABLE CAUSE

5. The United States is conducting a continuing criminal investigation of Michael Shearer regarding his sexual exploitation of children and receipt of child pornography.

6. Between approximately June 1, 2020, and July 27, 2020, Shearer, then a 37-year-old man, communicated online with a 15-year-old girl in Queens, New York (the "victim"), who sent Shearer several sexually explicit images of herself. The victim's mother reported the incident to the New York City Police Department on or about July 31, 2020. As

part of the investigation, the victim's mother consented to providing the victim's electronic devices. Law enforcement identified hundreds of messages between Shearer and the victim, including sexually explicit photographs of the minor victim.

7. Specifically, on or about June 2, 2020, the victim and Shearer using the SUBJECT ACCOUNT communicated on the social media application Discord. Shearer told the victim "You have me so hard …. I want you so bad right now." The victim responded with a shocked emoji. Shearer then asked, "Are you alone?" to which the victim responded "Yeah my parents are downstairs. Why?" Shearer asked, "Are you as aroused as I am?" The victim responded "Maybe" with a shocked emoji. Shearer then wrote to the victim that he would like "to guide" her "to do something to herself" and "It would make me feel so good to help you have an amazing orgasm." Shearer using the SUBJECT ACCOUNT then instructed the victim to masturbate, and he sent the victim a picture of his penis. Shearer using the SUBJECT ACCOUNT then asked to see a photo of the victim and asked for the victim's help orgasming. He wrote "Right now how close I am. Just send me pictures. Of you or things that are hot. I just want you so bad right now." In response to his request, the victim sent an image of her unclothed abdomen and pubic area.

8. Law enforcement also lawfully obtained Instagram records for accounts associated with Shearer and the victim. In Instagram messages on or about July 3, 2020, the victim sent Shearer approximately three photos of her nude body, showing her breasts and pubic area, amid a sexually charged conversation. In response to the photos, Shearer wrote to the victim "I want to bury my face between your legs and chest" and "I want you to sit on me now."

9. Shearer was aware that the sexually explicit photographs were of a minor. The victim informed Shearer on approximately June 2, 2020, that she was "about to turn 16."

10. On May 13, 2022, a grand jury in the Eastern District of New York returned a two-count indictment charging Shearer with receiving and producing child pornography in violation of 18 U.S.C. §§ 2251(a), 2251(e), 2252(a)(2), and 2252(b)(1).

11. On or about April 25, 2023, law enforcement interviewed an individual who is familiar with Shearer. He/she stated in sum and substance that Shearer is attracted to young teenagers, and that he would communicate with a lot of young people on Discord. He/she stated that he/she overheard flirtatious conversations.

12. On or about March 6, 2024, Discord provided non-content records pursuant to an order under 18 U.S.C. § 2703(d) related to the SUBJECT ACCOUNT. The records showed that the SUBJECT ACCOUNT contains over 600 messages communicating with various other accounts in about 2022. One of the "servers"[1] on which the SUBJECT ACCOUNT was communicating was called "Aftercare 18+." Based upon my training and experience, I understand a social media group with an 18+ label to mean that it contains sexually explicit or pornographic material.

13. Moreover, I understand that Shearer has a previous conviction related to child exploitation. In or about 2013, the defendant was convicted of unlawful transaction with a minor in Kentucky. Based on my review of criminal history records, I understand that the defendant was initially charged with prohibited use of electronic communication system to

[1] According to Discord, "servers" are the groups or spaces. They are made by specific communities and friend groups. The vast majority of servers are small and invitation-only. Some larger servers are public. Any user can start a new server for free and invite their friends to it. See What Is Discord, Discord (May 12, 2022), https://discord.com/safety/360044149331-what-is-discord

procure a minor for a sex offense, which was pleaded down to the unlawful transaction conviction.

14. In addition, based on my review of criminal history records, I understand that Shearer faces a charge of sexual abuse of minors in Kentucky. On or about July 8, 2022, the defendant was charged with first degree sexual abuse of two victims under 12 years of age in violation of Kentucky law. According to the complaint, the defendant sexually abused an 8-year-old victim, by forcing the victim to touch the defendant's penis. The defendant separately abused a different child by touching her breast and forcing the victim to touch the defendant's penis. When the defendant was arrested on these charges, on or about July 11, 2022, he attempted to flee from police. I understand that the case is still pending.

15. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and who produce, receive, or possess images of child pornography.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and

gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in a secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer, on social media applications, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

16. Based on the foregoing, including (a) Shearer's exploitation and receipt of child pornography using the SUBJECT ACCOUNT, (b) records from Discord indicating that the SUBJECT ACCOUNT has over 600 messages, (c) records that some of the messages in the SUBJECT ACCOUNT relate to "18+" servers and thus likely involve sexually explicit themes, (d) Shearer's history of child exploitation crimes, and (e) that persons with sexual interest in children or an interest in producing or collecting child pornography typically keep such images

for extended periods of time,[2] I submit there is probable cause to search the SUBJECT ACCOUNT, as described in Attachment A, for the things particularly described in Attachment B.

DISCORD AND ELECTRONIC COMMUNICATIONS SERVICES

17. Based on Discord's Privacy Policy, available online, I know the following about the collection and preservation of data at Discord.

a. Discord collects information from users when they voluntarily provide information, such as when they register for access to the Discord application and related Internet services (the "Services"). Information Discord collects may include, but is not limited to, username, email addresses, and any messages, images, transient VOIP data (to enable communications delivery only), or other content users send via the chat feature.

b. When the users interact with Discord by using its Services, Discord receives and stores certain information such as an IP address, device ID, and the user's Services activities. Discord may store this information in databases owned and maintained by affiliates, agents, or service providers. The Services may use this information and pool it with other information to track, for example the total number of visitors to Discord's website, the

[2] Indeed, several appellate courts have ruled that the staleness inquiry for search warrants differs in the child exploitation context. See United States v. Carroll, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); United States v. Seiver, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., United States v. Allen, 625 F.3d 830, 843 (5th Cir. 2010); United States v. Richardson, 607 F.3d 357, 370-71 (4th Cir. 2010); United States v. Lewis, 605 F.3d 395, 402 (6th Cir. 2010)); see also United States v. Hernandez, No. 19 CR 0097(VM), 2020 WL 3257937, at *23 (S.D.N.Y. June 16, 2020) (denying motion to suppress based in part on Carroll).

number of messages users have sent, and the domain names of the visitors' Internet service providers.

c. Discord uses cookies and similar technologies to keep track of users' local computer settings such as notification settings and which account users have logged into the services. Cookies are pieces of data that sites and services can set on a user's browser or device that can be read on future visits. In addition, Discord uses technologies such as web beacons and single-pixel gifs to record log data such as open rates for email sent by the system.

d. Discord may use third party website analytic tools such as Google Analytics on its website that use cookies to collect certain information concerning use of its Services. However, users can disable cookies by changing their browser settings.

18. Discord users are able to create and maintain a friends list, participate in multiple servers of communication channels, and set their current status indicator to appear online, away, or invisible, to other users. Discord servers can have multiple text-based and voice channels, both public and private. Text messages sent in these channels are persistent, stay visible, and are stored indefinitely. Users are able to communicate in only one channel at a time, but can easily navigate between channels. Discord users are able to direct message, or private message other Discord users. Discord users are able to view what game their Discord friends and other Discord server members are playing.

19. During the registration process for a Discord account, Discord asks subscribers to provide basic client information to include username and email address. Additionally, other online applications like Steam, Facebook, Spotify, and Twitter can be connected to a user's Discord account. Discord can be used from within a web browser, can be installed on a Windows, Mac, or Linux computer, or can be installed on an Apple iOS or

Android mobile device. Discord has an optional paid version called "Discord Nitro" which provides a user with additional features. Therefore, the computers of Discord likely contain information concerning a user's account and their use of Discord services and possibly other connected services, such as account access information, email information, and account application and payment information.

20. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like Discord, allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an email or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other email addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the users of an account.

21. Therefore, Discord's computers are likely to contain stored electronic communications and information concerning subscribers and their use of Discord's Services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute

evidence of the Subject Offenses because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

22. A subscriber of a service provider, such as Discord, can also store with the service provider files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to emails), notes, and other files, on servers maintained and/or owned by the service provider. In my training and experience, evidence of who was using an account may be found in such information.

23. In my training and experience, email and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as login into the account via the provider's website), and other log files that reflect usage of the account. In addition, email and social media providers often have records of the IP address used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help identify which computers or other devices were used to access the SUBJECT ACCOUNT.

24. In my training and experience, email and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of emails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any

actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

25. I know based on my training and experience that providers of email or social media services generally have access to and store the web or Internet browsing history of the user while he or she is logged into an account. That history can include names and specific websites or URLs/URIs of the sites that have been visited.

26. I know based on my training and experience that providers of email or social media services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI (web address), HTTP protocol version, referrer, and similar information, login tracker logs; account management logs; and any other email or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT. These can be used to determine the types of devices used while accessing the SUBJECT ACCOUNT as well as data related to the user's activity while accessing the SUBJECT ACCOUNT.

27. Users of accounts are often required to include an email account as well as a phone number in subscriber records. The e-mail account may be an email account hosted at the same provider, or an account at a different provider. The email account is referred to by several names, such as secondary email account, a recovery email account, or an alternative email account or communication channel. The email account is often used when the identity of the

user of the primary account (the target account) needs to be verified, for example if a password is forgotten, so that the provider can confirm that the person trying to access the account is the authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as "two-factor authentication" (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary email account and a secondary email account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary email account or to the phone number listed in subscriber records can allow access to the primary account.

28. Providers also frequently obtain information about the types of devices that are used to access accounts like the SUBJECT ACCOUNT. Those devices can be laptop or desktop computers, cellular phones, tables, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware modules, operating system versions, unique device identifiers, Global Unique Identifiers or "GUIDs," serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile

Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI") or International Mobile Equipment Identities ("IMEI"). Apple, one of the primary suppliers of mobile devices used to access accounts like the SUBJECT ACCOUNT, had previously used an identifier that was unique to the hardware of its devices, such that details of a device's activity obtained from a particular application or "app" could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still unique to a device, but which can be wiped and re-generated if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different apps or services.

29. These device identifiers can be used to (a) identify accounts accessed at other providers by the same device, and (b) determine whether any physical devices found during the investigation were the ones used to access the SUBJECT ACCOUNT. The requested Warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

30. Providers of email and social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in several ways. For example, a user may access the provider's services by running an application on the user's phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning ("GPS") information. It may also be accessible through "check-in" features that

some providers offer that allow users to transmit or display their location to their "friends" via the provider.

31. The subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly, rather they use an algorithm that is performed on the password and generate a new random string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashtag algorithm is performed on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some providers insert additional text before or after the password, which is referred to as "salting" the password. The hashtag algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively, or in addition to passwords, users may be required to select or propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user's password.

CONCLUSION

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Discord to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

33. Because the warrant will be served on Discord, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

RICHARD C STEPIEN

Digitally signed by RICHARD C STEPIEN
Date: 2024.03.11 18:07:11 -04'00'

Richard Stepien
Special Agent
Homeland Security Investigations

Sworn to me by telephone on March 13, 2024

Taryn A. Merkl

THE HONORABLE TARYN A. MERKL
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to the Discord account with username: DaddyWolf#1013 and user ID: 586605183941738513 (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Discord, an electronic communications and remote computer services provider headquartered in San Francisco, California.

ATTACHMENT B

I. Information to be Disclosed by Discord

To the extent that the information described in Attachment A is within the possession, custody, or control of Discord, including information that has been deleted but is still available, Discord is required to disclose the following information for the SUBJECT ACCOUNT listed in Attachment A, for the period of January 1, 2020 through July 30, 2022:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT including:

   i. All emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the SUBJECT ACCOUNT, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

   ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, voice and voice-over-IP data, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

   iii. All records pertaining to communications between Discord and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken;

   iv. All search history and web history, including web clicks or "History Events," by the user(s) of the SUBJECT ACCOUNT;

v. All web browsing activities that are identifiable with the SUBJECT ACCOUNT; and

vi. Any and all logs of user activity and user agent string including: web requests or HTTP requests; any logs containing information such as the requestor's IP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other email or social media accounts accessed or analytics related to the SUBJECT ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the SUBJECT ACCOUNT was created, the length of service, the IP address used to register the SUBJECT ACCOUNT, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the SUBJECT ACCOUNT, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and courses of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address

information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

1. The SUBJECT ACCOUNT;
2. Any other account associated with the SUBJECT ACCOUNT, including by means of sharing a common secondary, recovery or alternate email address listed in subscriber records for the SUBJECT ACCOUNT or by means of sharing a common phone number or SMS number listed in subscriber records for the SUBJECT ACCOUNT; and
3. Any other account accessed by a device with an identifier responsive to the device identifiers called for in section I.b.iii, below

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Attachment A, including log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups and locations;

iii. Any information identifying the device or devices used to access the SUBJECT ACCOUNT, including any Android ID, advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "UID" serial number, mobile network, subscriber information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic

Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module ("SIM"), Mobile Subscriber Identifier ("IMSI"), international Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDEFA"), and any other information regarding the types of devices used to access the SUBJECT ACCOUNT or other device specific information; and

iv. Any information showing the location of the user of the SUBJECT ACCOUNT, including while sending or receiving a message using the SUBJECT ACCOUNT or accessing or logged into the SUBJECT ACCOUNT.

Discord is hereby ordered to disclose the above information to the government within ten days of the issuance of this warrant.

II. Information to be Seized by the Government

For the account listed in Attachment A, the search team may seize all information described above in Section I that constitutes evidence, contraband, fruits, or instrumentalities of 18 U.S.C. § 2251(a) (sexual exploitation of a child); § 2422(b) (enticement to engage in sexual activity); and § 2252(a)(2) (receipt of child pornography), and attempt and conspiracy to commit those crimes (the "Subject Offenses"), and for the period of January 1, 2020 through July 30, 2022, information pertaining to the following matters:

a. Communications or records regarding pornography or exploitation;

b. Communications between the user of the SUBJECT ACCOUNT and other minors;

c. Information that constitutes evidence of the identification or location of the user(s) of the SUBJECT ACCOUNT;

d. Information that constitutes evidence concerning persons who either collaborated, conspired, or assisted in the commission of the criminal activity under investigation or communicated with the SUBJECT ACCOUNT about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

e. Information that constitutes evidence indicating the SUBJECT ACCOUNT user's or co-conspirator's state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning related to the criminal activity;

f. Information that constitutes evidence concerning how and when the SUBJECT ACCOUNT was accessed or used to determine the geographic and chronological context of account access use and events relating to the crime under investigation and to the SUBJECT ACCOUNT's user;

g. Current and historical friends lists, stating all full-case sensitive usernames including any user IDs associated with their usernames; and

h. List of users the SUBJECT ACCCOUNTS have communicated with.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may

deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.